REMARKS

In the Office Action, dated January 4, 2005, the Examiner states that Claims 1-13 are pending and Claims 1-13 are rejected. By the present Amendment, Applicant amends the claims.

In the Office Action, Claim 2 is objected to for a minor informality, which the Applicant has now attended to.

In the Office Action, Claims 4, 7 and 10 are rejected under 35 U.S.C. §102(e) as being anticipated by Mapson (WO 98/32260). Claims 1-3, 5, 6, 8, 9 and 11-13 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mapson in view of Nixon et al. (US 5,828,851). The Applicant respectfully disagrees with and traverses these rejections.

Claim 4 of the present application recites a method for reception of a securely transmitted message by a recipient device the method comprising the steps of: (i) extracting one or more of a device identifier, an application identifier and an application value from a received secure message; (j) generating by a first process using the device identifier, the application identifier and the application value a message value; (k) generating, according to a second process using the device identifier and the application identifier one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message; (l) combining the message value with the one or more secret values, to establish a secret message value; (m) extracting a secure message block from the secure message; and (n) applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

From a terminology perspective, the device identifier DID is a unique identifier allocated to a particular device (page 12 lines 3-6). The application identifier AID is used to identify the particular software application that is involved in the secure transaction being considered (page 10 lines 23-25). The application value AUV is used for auditing and indexing purposes and is assigned to each message transmitted (page 13 lines 20-23). The secret values SV are, as recited in the claim known substantially only to an originating device and the one or more intended recipient devices of the message.

As depicted in Figs. 5 and 6 the AUV, AID, DID, and SV are processed together with the message date 600 to form a transmission data block 606. The transmission data block 606 takes the form of three major components, namely the secure message block 604 (SMB), control date 610, and addressing data 612 (page 15 lines 19-21). The secure message block (SMB) 604 is opaque, that is indecipherable, to all network entities apart from the intended recipient (page 15 lines 26-28). The Issuer device 200 and the device-holder device 202 are arranged to allow one or more secret values 400 known only to the Issuer's device 200 and the device-holders device 202 to be stored in both the Issuer device 200 and the device-holder device 202 (page 11 lines 8-11). Accordingly, as depicted in Figs. 8 and 9, the DID, AID and AUV are processed to retrieve the SV at 400, and the message data at 600.

Mapson uses a single identifier B1 to identify how a message is secured, and a second identifier T1 inside the secured message to test for duplicated messages. Mapson discloses a device master key B1 (Fig. 2) that is loaded into the secure device (page 8 lines 17-24). This is equivalent to the DID in the present application. Mapson also discloses a sequentially incremented device transaction number T1 (Fig. 2, page 8 lines 30-31). This is equivalent to the AUV of the present application.

The acquirer in Mapson determines from the unencrypted Secure Device Identifier B1 which institution issued the secure device (page 6 lines 8-11) and forwards the transaction to the secure device issuer (page 6 lines 12-14). The secure device issuer decrypts the certificate data and checks the transaction number (ie T1) against a transaction number database to determine if it is valid. This validity check involves checking if T1 is one of the possible transaction numbers for the particular device, and if the transaction number has not been used before (page 6 lines 15-20). The entire transaction is then sent to the acquirer for normal processing (page 6 lines 20-21).

Mapson thus does not disclose or suggest use of the application identifier AID or the secret values SV. Use of the AID enables a device using the method of claim

4 to be used for multiple purposes or applications, something not possible according to Mapson. Use of the SV, which is known only to the Issuer's device 200 and the device-holders device 202, enables the aforementioned pair of devices to exchange secured information without requiring the additional involvement of a third part (ie the secure device issuer).

From another perspective, Mapson uses a second identifier inside the secured message to identify the message. In contrast, the arrangement recited in claim 4 uses several identifiers outside the secured message block to determine how the specific message is secured while identifying the message.

In summary, having regard to claim 4 of the present application, Mapson does not disclose or suggest generating by a first process using the device identifier, the application identifier and the application value a message value; or (k) generating, according to a second process using the device identifier and the application identifier one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message; or (l) combining the message value with the one or more secret values, to establish a secret message value; or (m) extracting a secure message block from the secure message; or (n) applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

Accordingly, claim 4 of the present application is considered novel over Mapson. Claims 7 and 10 recite the same or equivalent features to those in claim 4, and accordingly, those claims too are considered novel over Mapson.

In paragraph 6, the Office Action concedes that Mapson does not explicitly disclose "combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value" (ie feature (d) of claim 1 of the present application) and refers to Nixon in this regard.

Nixon is directed to "process control systems....for controlling...devices of multiple different types..." (Column 2 lines 3-8). Nixon describes, in relation to Fig. 2, a control model and a run time model which download a Device Table in order to interconnect the aforementioned models (Column 9 lines 46-61). Device tables contain "....information regarding a device in the process control environment...including a device ID, a device name, a device type, a Process Control Network (PCN) network number, an Area Controlled Network (CAN) segment number, a simplex, redundant communication flag, a controller MAC address, a comment field, a primary internet protocol (IP) address, a primary subnet mask, a secondary IP address and a secondary subnet mask." (Column 10 line 63 – Column 11 line 2). The Device Table is downloaded on start-up and when the Device Table is changed, and for the example of a controller/multiplexer, includes only data for devices for which the controller/multiplexer is to initiate communications (Column 9 lines 60-64).

Even allowing for the assertion that Nixon discloses a combination of addresses and device characteristics, Nixon is not concerned with secure communications, and neither discloses nor suggests at least the features, from claim 1, of combining a message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value; or applying the secret message value and the message to an encoding process to form a secure message block; or combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

Establishment of prima facie case of obviousness requires that the prior art reference (or references when combined) must teach or suggest all the claim limitations. Even supposing that Mapson were to be modified by incorporating the Device Table of Nixon, this would still not teach or suggest all the claim limitations of claim 1, since neither Mapson nor Nixon recite the features of that claim noted above. In order to modify the combination of Mapson and Nixon to arrive at claim 1 of the present Invention it would be necessary to modify the combination to incorporate at least the features combining a message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value; and applying the secret message value and the message to an encoding process to form a secure message block; and combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

In conclusion, it is submitted that for at least the reasons noted, even if Mapson and Nixon are combined, claim 1 is considered patentable over the noted citations whether these are taken individually or in combination. The other claims rejected the Office Action recite the same or equivalent features to those of claim 1. It is thus submitted that for at least the reasons noted, even if Mapson and Nixon are combined, those claims too are patentable over the noted citations whether these are taken individually or in combination.

In light of the foregoing response, all the outstanding objections and rejections are considered overcome. Applicant respectfully submits that this application should now be in condition for allowance and respectfully requests favorable consideration.

Respectfully submitted,

April 1, 2005
Date

Attorney for Applicant
Brian W. Hameder
c/o Ladas & Parry LLP
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300
Reg. No. 45613